



Office of the Governor
State Chief Information Officer

Introduction for Statewide Information Security Manual

The Statewide Information Security Manual is the foundation for information technology security in North Carolina. It sets out the standards required by G.S. §147-33.110, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets.

The Manual is based on industry best practices and follows the International Organization for Standardization Standard 17799 (ISO 17799) for information technology security. The standards have been extensively reviewed by representatives of each agency within the executive branch of state government and are continuously reviewed as technology and security needs change.

The Statewide Information Security Manual sets forth the basic information technology security requirements for state government. Standing alone, it provides each executive branch agency with a basic information security manual. Some agencies may need to supplement the manual with more detailed policies and standards that relate to their operations and any applicable statutory requirements, such as the Health Insurance Portability and Accountability Act of 1996 and the Internal Revenue Code. To assist agencies in their compliance with the state manual and in developing their own unique standards, the North Carolina Office of Information Technology Services (ITS) has licensed both ISO 17799 and its accompanying toolkit for all agencies covered by the security standards law. The Enterprise Security and Risk Management Office staff is available to answer any questions related to the Statewide Information Security Manual and to assist agencies in meeting their unique needs.

Guidance for Agencies

While this Manual is the foundation for information technology security in state government, simply adopting these standards will not provide a comprehensive security program. Agency management should emphasize the importance of information security throughout their organizations with ongoing training and sufficient personnel, resources and support.

Implementation and Management

Agency heads should also consider periodic internal and external reviews of their information security program. The reviews may be staggered but should collectively include technical security controls, such as devices and networks, and non-technical security controls, which include policies, processes, and self-reviews. Independent information security reviews should also be considered when there are significant changes to the agency's information security posture because of a technology overhaul, significant change in business case or information protection needs.

ISO 17799: 2005 REFERENCE

- 6.1.1 Management commitment to information security
- 6.1.2 Information security coordination
- 6.1.3 Allocation of information security responsibilities
- 6.1.8 Independent review of information security